ALB

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

UNITED STATES OF AMERICA

- against -

THE PREMISES KNOWN AND DESCRIBED AS 68 FOSTER AVE, VALLEY STREAM, NEW YORK 11580 AND ANY DEVICES CAPABLE OF ACCESSING THE INTERNET ON THE PERSON OF JOHN CAPUANO

----------X

TO BE FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

M. No. _____
(18 U.S.C. §§ 2252 and 2252A)

MJ 15-0479

AKT

DEBRA GERBASI, being duly sworn, deposes and says that she is a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is kept and concealed within THE PREMISES KNOWN AND DESCRIBED AS 68 FOSTER AVE, VALLEY STREAM, NEW YORK 11580 (hereinafter referred to as the "SUBJECT PREMISES") AND ANY DEVICES CAPABLE OF ACCESSING THE INTERNET ON THE PERSON OF JOHN CAPUANO (hereinafter the "SUBJECT DEVICES"), the items described in Attachment B to this affidavit, all of which constitute evidence or instrumentalities of the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Section 2252 and 2252A.

The source of my information and the grounds for my belief are as follows:[1]

---

[1] Because the purpose of this Affidavit is to set forth only those facts necessary to

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

1. I have been employed as a Special Agent with the Department of Homeland Security since 2002, and am currently assigned to the Child Exploitation Group ("CEG"). I have gained expertise in the conduct of child pornography and exploitation investigations through training in seminars, classes, and daily work related to conducting these types of investigations, including the execution of multiple search warrants relating to child pornography offenses and the subsequent prosecution of offenders.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. I am investigating the activities of a person who used a computer connecting to the Internet to transport, receive, access with intent to view and possess child pornography, in violation of Title 18, United States Code, §§ 2252 and 2252A. As will be shown below, there is probable cause to believe that fruits, evidence and instrumentalities of the unlawful transportation, receipt, access with intent to view and possession of child pornography are located at the SUBJECT PREMISES and in the SUBJECT DEVICES. I am submitting this affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES and the SUBJECT DEVICES, which are more particularly described in Attachment A, and the seizure of the items more particularly described in Attachment B.

4. All information contained in this affidavit is either personally known by me or has been related to me by other law enforcement agents. Since this affidavit is being submitted for

---

establish probable cause to search, I have not set forth all of the facts and circumstances of which I am aware.

the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, U.S.C. §§ 2252 and 2252A, are presently located at the SUBJECT PREMISES and in the SUBJECT DEVICES. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of Title 18, United States Code, §§ 2252 and 2252A, relating to material involving the sexual exploitation of minors. Title 18, United States Code, Section 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, accessing with intent to view or possessing any visual depiction of a minor engaging in sexually explicit conduct when such visual depiction was either mailed or, using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce. Title 18, United States Code, Section 2252A(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, accessing with intent to view or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or, using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched.

Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

k. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

l. An Internet Service Provider (ISP) is a commercial service that provides Internet connectivity to its subscribers. In addition to providing access to the Internet via telephone lines or other telecommunications lines/cables, ISPs may also provide Internet e-mail accounts and other services unique to each particular ISP such as Usenet (newsgroups) and chat/messaging functions. ISPs maintain records pertaining to the individuals or companies that

have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, customer service information and other information, both in computer data format and in written record format.

m. A "server" is a centralized computer that provides services for other computers connected to it via a network. The computers that use the server's services are sometimes called "clients."

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

7. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

8. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

9. Child pornographers can transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With digital cameras the images can be transferred directly onto a computer. A computer can connect to another computer through the

use of telephone, cable, or wireless connections. Electronic contact can be made to literally millions of computers around the world.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

11. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

12. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

13. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to

electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

Kik Messenger Application

14. The Kik Messenger application is primarily a social media mobile device platform designed and managed by Kik Interactive Incorporated, a Waterloo, Canada based company, for the purpose of mobile messaging and communication. To use this application, a user downloads the mobile messaging application via an applications service such as the Google Play Store, Apple ITunes, or other similar mobile application provider. Once downloaded and installed, the user is prompted to create an account and a username. This username will be the primary account identifier. The user also has a display name, which will be what other users initially see when transmitting messages back and forth. As part of the account creation process, Kik users are asked to supply a valid email address, create a password, provide an optional date of birth, and user location. The user also has the option of uploading a "profile avatar" that is seen by other users Once the Kik user has created an account, the user is able to locate other users via a search feature. The search feature usually requires the user to know the intended recipient's username. Once another user is located or identified, Kik users can send messages, images, and videos between the two parties.

15. Kik Messenger also allows users to create chat rooms, of up to 50 people, for the purpose of communicating and exchanging images and videos. These rooms are administered by the creator who has the authority to ban and remove other users from the created room.

According to Kik Messenger, more than 40% of the Kik users chat in "groups" and approximately 300,000 new groups are created every day. These groups are frequently created with a "hashtag" allowing the group or chat to be identified more easily. Once the group or chat is created Kik users have the option of sharing the "link" with all of their contacts or anyone they wish.

16. Kik Messenger users frequently advertise their Kik usernames on various social networking sites in order to meet and connect with other users. In some cases, Kik also provides various avenues, such as dating sites and social media applications, for meeting other users. HSI undercover agents have observed, in various chats, that many of the users stated they felt safe using Kik Messenger as a means of trading child pornography and for other illegal activities due to the fact that "Kik is a Canadian based company and not subject to the same United States laws." HSI undercover agents have also noted messages posted in Kik Messenger chat rooms relating to the enforcement, deletion, or banning of users and rooms by Kik Messenger for the purpose of exchanging or distributing child pornography. HSI agents noted the comments to include the continued creation of new rooms and new user accounts to circumvent Kik Messengers enforcement efforts.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

17. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

16. To fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware

drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

17. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, printer, modem, router, or any other computer hardware or software or mobile Internet devices found at the SUBJECT PREMISES and the SUBJECT DEVICES are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251 through 2256, and should all be seized as such.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

18. Over the course of my law enforcement career, Your Affiant has conducted a significant number of investigations concerning online child sexual exploitation, focusing specifically on crimes involving child pornography. Your Affiant has personally interviewed a large number of child sex offenders who committed online child pornography crimes. Your Affiant also has been informed of the studies of child sex offenders in general, and child pornography offenders in particular. Your Affiant also has learned about the activities and characteristics of child pornography offenders from other law enforcement agents who focus on online child sexual exploitation, including those who investigate the offenses and those who analyze the computer equipment of the offenders.

19. Based on my own experience and what I have learned from other individuals who specialize in the investigation and study of child pornography offenders, I know that the following traits and characteristics are generally found to exist and be true in cases involving individuals who collect child pornography:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar platforms.

d. Individuals who collect child pornography sometimes also maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of

persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. The majority of individuals who collect child pornography rarely dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials.

20. Based on my own experience in investigating computer-facilitated child sexual exploitation crimes, and the experiences of other law enforcement agents with who I have consulted, I believe that the majority of individuals who collect child pornography via the Internet maintain their collections, increasingly in both online and offline storage media, as well as one hard drives of devices and in cloud or other types of virtual or remote storage locations. Doing so allows them to access and maintain their contraband collection even as they move from one physical location to another.

BACKGROUND OF THE INVESTIGATION

21. On April 19, 2015, an HSI Special Agent in Delaware acting in an undercover capacity signed into a Kik user account in order to conduct child exploitation investigations on the Kik Messenger application.

22. On April 19, 2015, at approximately 5:00 P.M. EST, this undercover special agent, using a device connected to the Internet, signed into undercover Kik Messenger account and saw that user "sorry8787" (Displaying the name "John") had posted at least five images and one video of child related sexually explicit material in the Kik Messenger chat room "#YoungFunzz"

on April 17, 2015, at approximately 11:18 A.M. The undercover special agent was able to download and save these images and video to an undercover device. These items included the following:[2]

a. A video file uploaded by sorry8787 at approximately 11:18:23 A.M. EDT, which shows a prepubescent girl approx. 4-7 years' old with her legs spread while tied to a bed and being penetrated from behind by an adult male;

b. A still image uploaded by sorry8787 at approximately 12:05:44 A.M. EDT, which shows the vaginal area of a prepubescent girl approx. 3-5 years' old with her underwear being pulled down by the hand of an adult male and ejaculation on here torso; and

c. A still image uploaded by sorry8787 at approximately 12:08:35 A.M. EDT, which shows a prepubescent girl approx. 8-10 years' old performing oral sex on an adult male.

23. On April 15, 2015, a U.S. Immigration and Customs Enforcement summons was served on Kik relating to the user "sorry8787" (Displaying the name "John").

24. On April 17, 2015, Kik responded to the subpoena and identified the user subscriber account with the following account information:

User name: sorry8787
First name: John
Last name:
Email: prosty@gmail.com (unconfirmed)
IP's used: 69.124.77.205
Location: US
Registered: 2015/02/13 08:36:39
Device: IPhone

---

[2] I have brought these images and the video file to show to United States Magistrate Tomlinson, and I ask that Judge Tomlinson initial here AKT to indicate that she reviewed these items prior to approving the requested warrant. These items will hereafter be stored by HSI.

25. A U.S. Immigration and Customs Enforcement summons was served on Cablevision, dba Optimum Online, relating to IP address 69.124.77.205 used to access the sorry8787 account on the Kik Messenger application.

26. On May 12, 2015, Cablevision responded to the summons and identified the subscriber account to which the target IP address 69.124.77.205 was assigned at the time of the uploads by sorry8787 as: "Dawn Capuano, 68 Foster Ave, Valley Stream, NY 11580." The information showed that the account was currently active and had been since May 7, 2000 and listed email address/user ids of "jcapuano@optonline.net" and, "jcapuano23@optimum.net."

27. On May 20, 2015, using a publicly available information, it was determined that the address at 68 Foster Ave, Valley Stream, NY 11580 listed a John and Dawn CAPUANO as residents.

28. A check of New York State Department of Motor Vehicle records on May 20, 2015 showed that John A. CAPUANO and Dawn L. CAPUANO have New York driver's licenses and vehicles registered at the SUBJECT PREMISES.

SPECIFICS REGARDING THE SEARCH AND SEIZURE OF NON-COMPUTER ITEMS

29. In addition to seizing any computer(s) and related devices and media found at the SUBJECT PREMISES, there is probable cause to belief that older, pre-digital child pornography and other child pornography related non-computer items (detailed in Attachment B) may be present at the SUBJECT PREMISES. Based on my consultations with experienced child exploitation agents investigating child pornography cases, viewers of child pornography often collect the pornography, amassing large collections over an extended period of time. Given the

characteristics of child porn viewers/collectors, I believe the SUBJECT PREMISES is likely to have magazines, books, photographs, motion pictures, films, videos, and other recordings of visual depictions of minors involving in sexual acts. I have been informed that investigators have often come across such items when executing computer-based search warrants. In addition, the sheer size of child pornography internet files makes it difficult for the child pornography viewer/collector to maintain these files solely on his/her computer. Thus, when executing search warrants in child porn cases, agents have often found CDs, DVDS, thumb drives, and other alternate forms of portable storage devices on which the child porn viewer/collector has stored the illicit items.[3] In addition, agents have often found handwritten notations in notebooks, etc., where the child pornography viewer/collector has written various IP addresses of child porn internet sites, so that he/she may easily visit the site again. It is also the experience of these agents that individuals who collect and trade video images of child pornography such as described herein nearly always also collect still images depicting minors engaged in sexually explicit conduct. Moreover, such individuals also use written notes or printouts related to their internet activity concerning child pornography, including, but not limited to passwords, lists of websites, filenames or lists of child pornography series.

---

[3] I understand from experienced investigators that individuals who collect child pornography typically have multiple computers and other devices capable of accessing or storing child pornography (in fact, most residences now how multiple devices capable of accessing the internet and storing images). Investigatively, there is no way to determine prior to forensic examination, which device accessed a given IP address under investigation or whether child pornography has been moved from that device into another device. As such, it is necessary to search any device capable of accessing or storing child pornography. Given the state of current technology, virtually any object may be such a repository for child pornography. For instance, pens, watches, mobile phones, MP3 players, video game systems and digital cameras are all examples of devices which may be used to store digital images of child pornography. Moreover, such devices meet the definition of a "computer" pursuant to Title 18, United States Code, Section 1030(e)(1). Finally, I note that iPhones are commonly backed-up onto computers kept in the residence.

REQUEST TO SEARCH

36. Based upon the facts set forth above, I believe that the user of the Kik Account "sorry8787" is a collector of child pornography[4] and there is probable cause to believe that the items listed on Attachment B hereto, which is incorporated herein by reference, will be found at the SUBJECT PREMISES and in the SUBJECT DEVICES, and that those items constitute evidence or fruits or instrumentalities of the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A.

37. It is further requested that this Affidavit be sealed by the Court until such time as the Court directs otherwise. Given the confidential nature of this investigation, disclosure would severely jeopardize the investigation in that it might alert the target of the investigation to the existence of an investigation and likely lead to the destruction and concealment of evidence, and/or flight.

WHEREFORE, your deponent respectfully requests that the Court issue a search

[4] Particularly I would note that individuals who post images (as opposed to more passively consuming images) are more likely to be collectors of child pornography. Moreover, the child pornography images here depict very young children and include bondage. These images are unlikely to be in the possession of an individual other than a serious collector of child pornography. Finally, these images had to be saved to a computer or mobile Internet device in order to be uploaded by the user to the Kik message board.

warrant for items listed in Attachment B of this affidavit, which is incorporated by reference as if fully set forth herein.

Debra Gerbasi

Special Agent Debra Gerbasi
Department of Homeland Security
Homeland Security Investigations

Sworn to before me this
21st day of May, 2015

/s/ A. Kathleen Tomlinson

THE HONORABLE A. KATHLEEN TOMLINSON
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

UNITED STATES OF AMERICA

- against -

THE PREMISES KNOWN AND DESCRIBED AS 68 FOSTER AVE, VALLEY STREAM, NEW YORK 11580 AND ANY DEVICES CAPABLE OF ACCESSING THE INTERNET ON THE PERSON OF JOHN CAPUANO

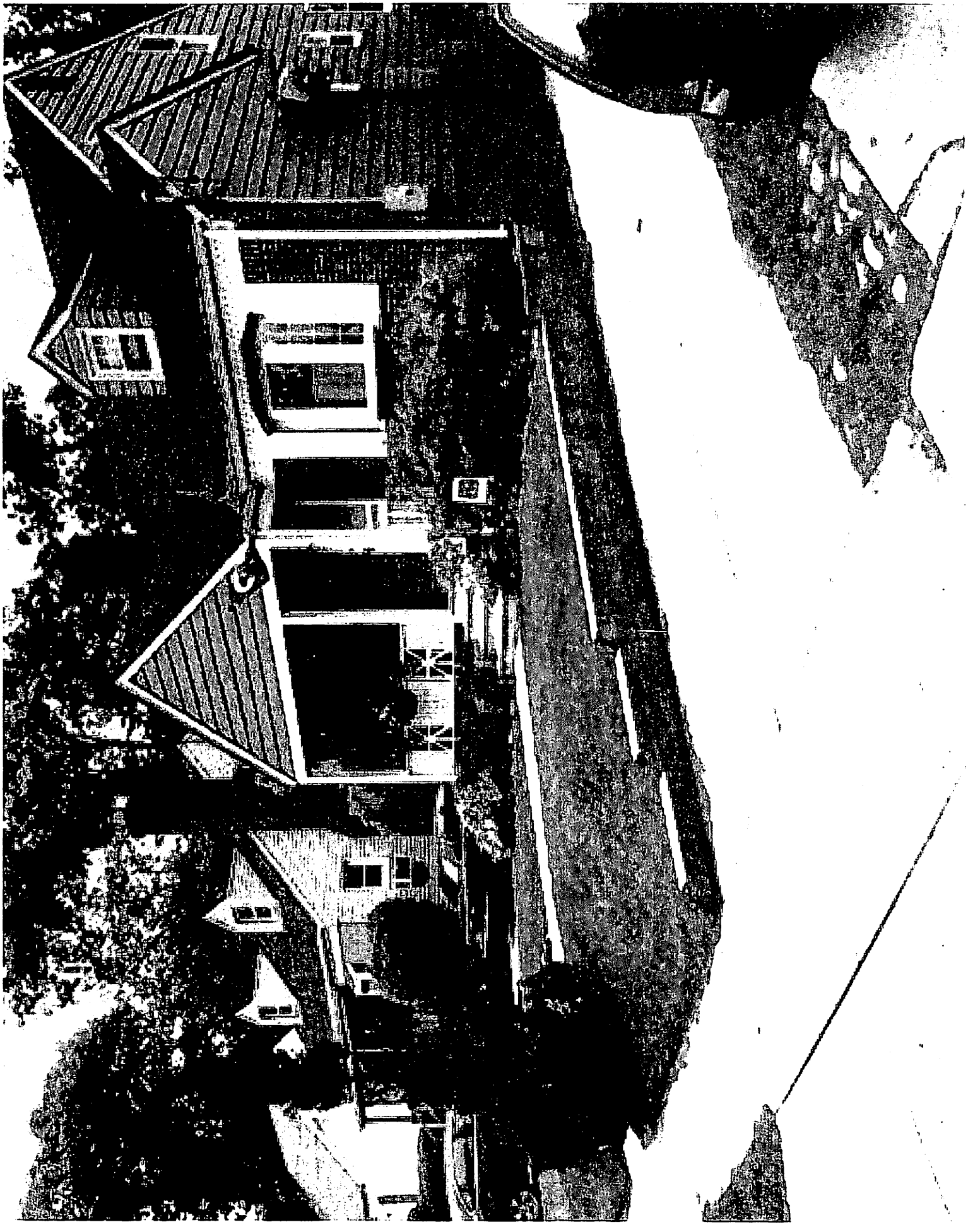
----------X

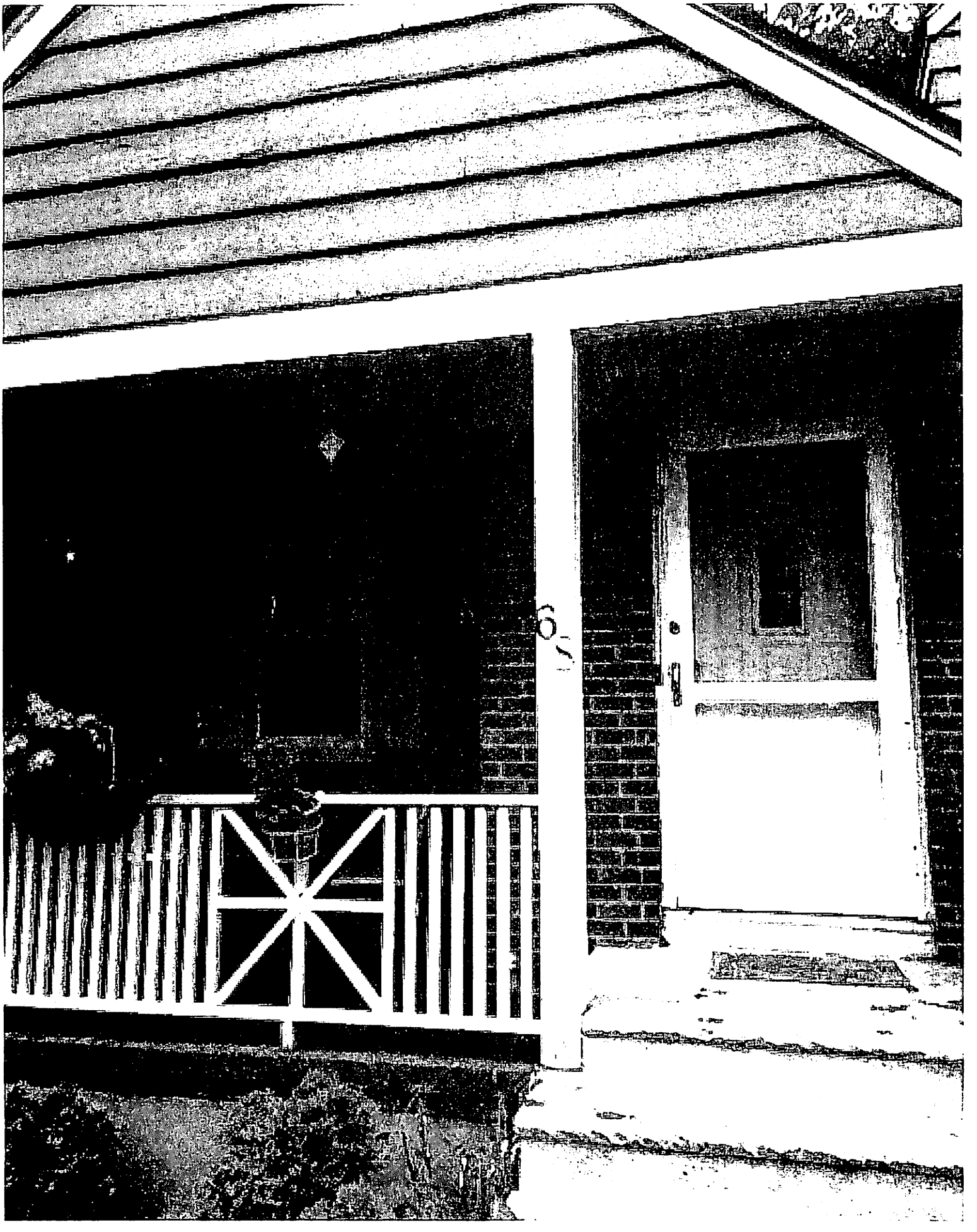
ATTACHMENT A

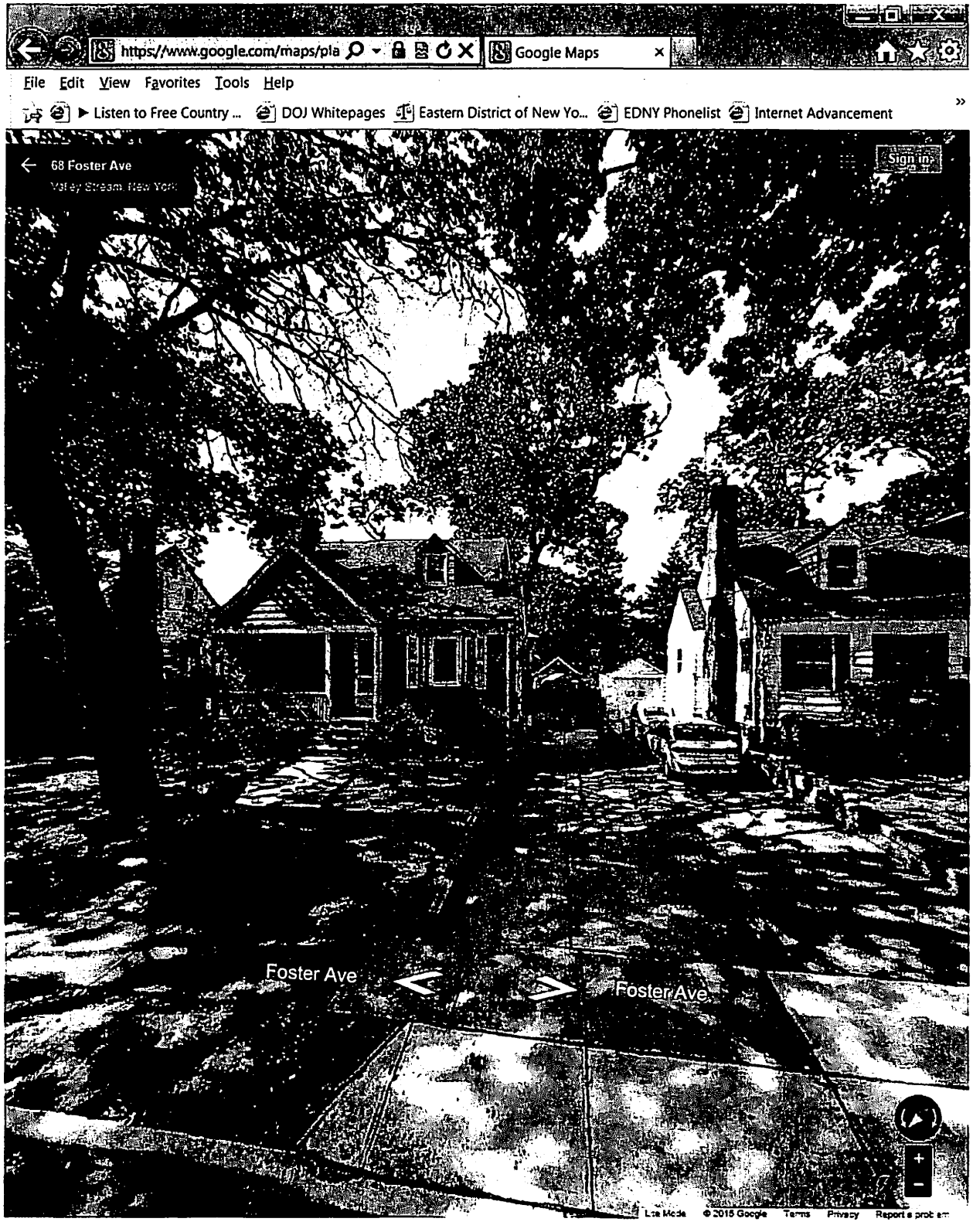
DESCRIPTION OF LOCATIONS TO BE SEARCHED

The SUBJECT PREMISES is located at 68 FOSTER AVE, VALLEY STREAM, NEW YORK, located between Cornwell Ave and Irving Place. The SUBJECT PREMISES appears to be a one family, two-story, cape-style residence with a concrete driveway on the right side of the house. The residence has a front porch with a white railing to the left of the front door. The SUBJECT PREMISES has light blue/gray siding and red brick exterior. The number "68" appears on a post near the front door. Photographs of the SUBJECT PREMISES are attached.

This warrant further authorizes the search of ANY DEVICES CAPABLE OF ACCESSING THE INTERNET ON THE PERSON OF JOHN CAPUANO.






https://www.google.com/maps/pla
Google Maps
File Edit View Favorites Tools Help
Listen to Free Country ...
DOJ Whitepages
Eastern District of New Yo...
EDNY Phonelist
Internet Advancement
68 Foster Ave
Sign in
Foster Ave
Foster Ave
© 2015 Google
Terms
Privacy

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

UNITED STATES OF AMERICA

- against -

THE PREMISES KNOWN AND DESCRIBED AS 68 FOSTER AVE, VALLEY STREAM, NEW YORK 11580 AND ANY DEVICES CAPABLE OF ACCESSING THE INTERNET ON THE PERSON OF JOHN CAPUANO

----------X

ATTACHMENT B

ITEMS TO BE SEIZED

A. Images of child pornography or child erotica; files containing images; and data of any type relating to the sexual exploitation of minors, in any form wherever it may be stored or found including, but not limited to:

i. Any cellular or mobile telephone or Internet device, personal digital assistant, computer, computer system and related peripherals; computer hardware; computer software; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, monitors, printers, external storage devices, routers, modems, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to computer passwords and data security devices and computer-related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

ii. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors;

iii. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors; and

iv. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors;

B. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors, that were transmitted or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors; and

ii. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors;

iii. Any and all records, documents, or materials, including any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors;

iv. Any and all records, documents, or materials, including any and all address books, names, and lists of names and addresses of minors visually depicted while

engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors;

v. Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums, including CDs or DVDs;

vi. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;

vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and

viii. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software;

C. Information, correspondence, records, documents or other materials pertaining to any child who has been present in the SUBJECT PREMISES, either in connection with the provision of childcare services or otherwise.

D. Credit card information including but not limited to bills and payment records, including but not limited to records of internet access;

E. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;

F. Records or other items which evidence ownership or use of computer equipment or any of the devices described in this attachment that are found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes;

G. Any and all adapters, chargers or other hardware items necessary to charge the battery, or to maintain the functioning of, any of the equipment described above; and

H. Any data or materials establishing ownership, use or control of any computer equipment seized from the SUBJECT PREMISES.